OWASP Day IV: introduzione

Matteo Meucci

OWASP-Italy Chair
CEO Minded Security

OWASP-Italy Day IV
Milan
6th, November 2009

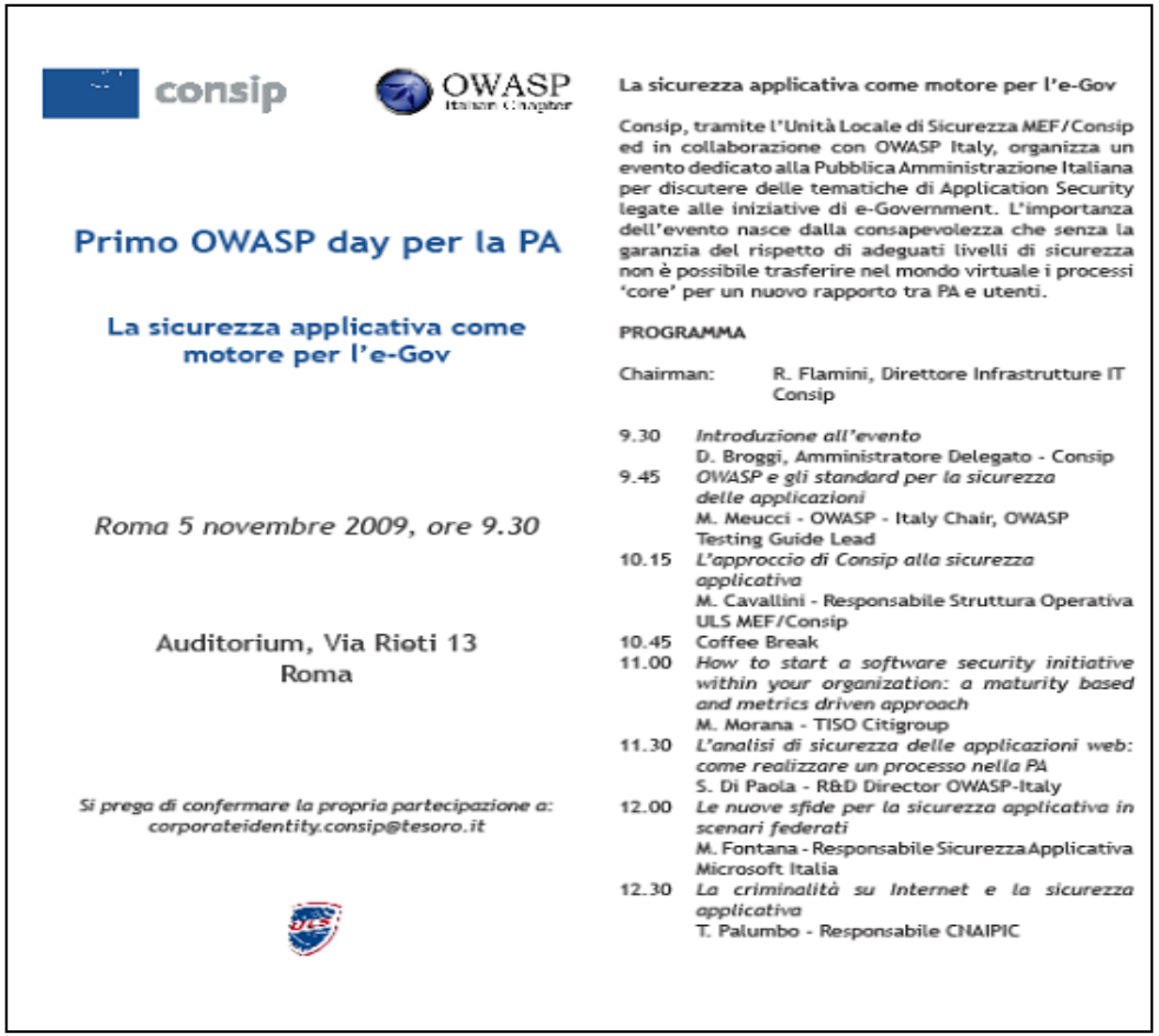
The OWASP Foundation
http://www.owasp.org

Who am I?

- Research
  - OWASP-Italy Chair
  - OWASP Testing Guide Lead

- Work
  - CEO @ Minded Security
    Application Security Consulting
  - 8+ years on Information Security
    focusing on Application Security

OWASP Day per la PA 2009



consip

OWASP Italian Chapter

Primo OWASP day per la PA

La sicurezza applicativa come motore per l'e-Gov

Roma 5 novembre 2009, ore 9.30

Auditorium, Via Rioti 13
Roma

Si prega di confermare la propria partecipazione a:
corporateidentity.consip@tesoro.it

La sicurezza applicativa come motore per l'e-Gov

Consip, tramite l'Unità Locale di Sicurezza MEF/Consip ed in collaborazione con OWASP Italy, organizza un evento dedicato alla Pubblica Amministrazione Italiana per discutere delle tematiche di Application Security legate alle iniziative di e-Government. L'importanza dell'evento nasce dalla consapevolezza che senza la garanzia del rispetto di adeguati livelli di sicurezza non è possibile trasferire nel mondo virtuale i processi 'core' per un nuovo rapporto tra PA e utenti.

PROGRAMMA

Chairman: R. Flamini, Direttore Infrastrutture IT Consip

9.30 *Introduzione all'evento*
D. Broggi, Amministratore Delegato - Consip

9.45 *OWASP e gli standard per la sicurezza delle applicazioni*
M. Meucci - OWASP - Italy Chair, OWASP Testing Guide Lead

10.15 *L'approccio di Consip alla sicurezza applicativa*
M. Cavallini - Responsabile Struttura Operativa ULS MEF/Consip

10.45 Coffee Break

11.00 *How to start a software security initiative within your organization: a maturity based and metrics driven approach*
M. Morana - TISO Citigroup

11.30 *L'analisi di sicurezza delle applicazioni web: come realizzare un processo nella PA*
S. Di Paola - R&D Director OWASP-Italy

12.00 *Le nuove sfide per la sicurezza applicativa in scenari federati*
M. Fontana - Responsabile Sicurezza Applicativa Microsoft Italia

12.30 *La criminalità su Internet e la sicurezza applicativa*
T. Palumbo - Responsabile CNAIPIC

OWASP - Italy Day IV

"Secure Software Initiatives"

6th November 2009, Milan

9:00	**Registration**
9:30	**"Introduction to the OWASP-Day"** Matteo Meucci - OWASP-Italy Chair
9:50	**"How to Create Business cases for Your Software Security Initiative"** Marco Morana — CISO, Citigroup
10:30	**"OWASP SAMM / Open Software Assurance Maturity Model"** Claudio Merloni — Software Security Consultant, Fortify Software
11:10	**Coffee break**
11:40	**"From Web Attacks to Malware. Can Secure Software Development Help Internet Banking Security?"** Giorgio Fedon — COO, Minded Security
12:20	**"Usability versus security: securing Internet facing applications while keeping them highly attractive for everybody" (ENG)** Tobias Christen — CTO, DSwiss Ltd
13:00	**Business Lunch**
14:00	**"NoScript, CSP and ABE: When the Browser Is Not Your Enemy"** Giorgio Maone — CTO, InformAction
14:40	**"Building Security In Maturity Model: A Review of Successful Software" (ENG)** Gabriele Giuseppini — Technical Manager, Cigital
15:20	**"The art of code reviewing"** Paolo Perego — Senior Consultant, Spike Reply
16:00	**Round Table: Why Software Security is not a priority in our digital world?** **M. Morana, C. Merloni, G. Giuseppini, S. Di Paola, M.Bregolin — Keynote R. Chiesa**

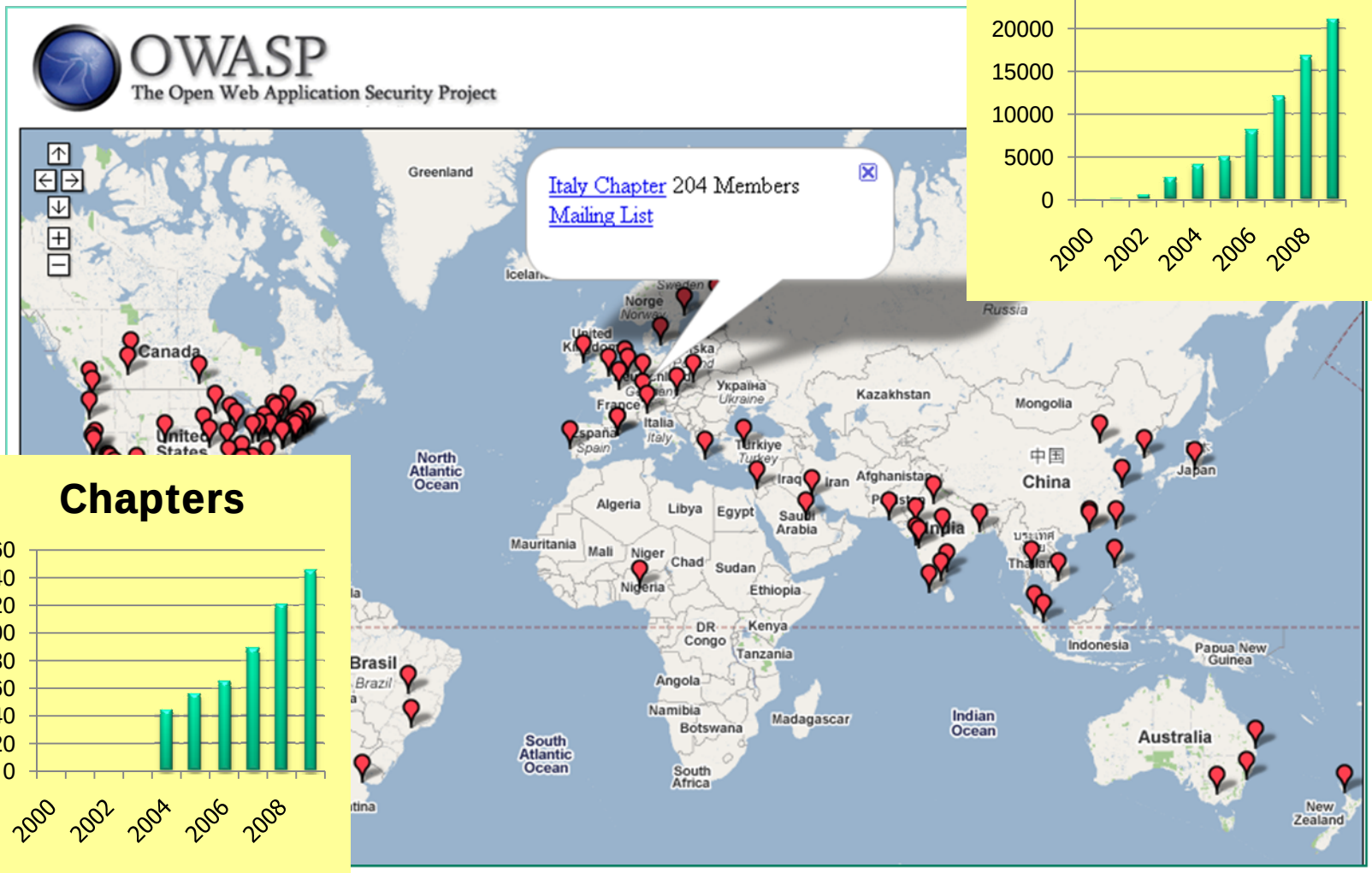
Certificazione CSSLP di ISC2

OWASP: The Open Web Application Security Project

OWASP
The Open Web Application Security Project

- Il progetto Open Web Application Security Project (OWASP) è una organizzazione Open Source dedicata alla creazione e alla diffusione di una cultura per quanto riguarda la sicurezza delle applicazioni web
- Progetto free, come il materiale disponibile sul portale www.owasp.org
- Migliaia di membri, +100 capitoli locali e altri partecipanti ai progetti. Milioni di hit su www.owasp.org al mese
- Defense Information Systems Agency (DISA) , US Federal Trade Commission (FTC), VISA, Mastercard, American Express e molte aziende in Italia hanno adottato la documentazione OWASP nei loro standard e linee guida

OWASP Worldwide Community

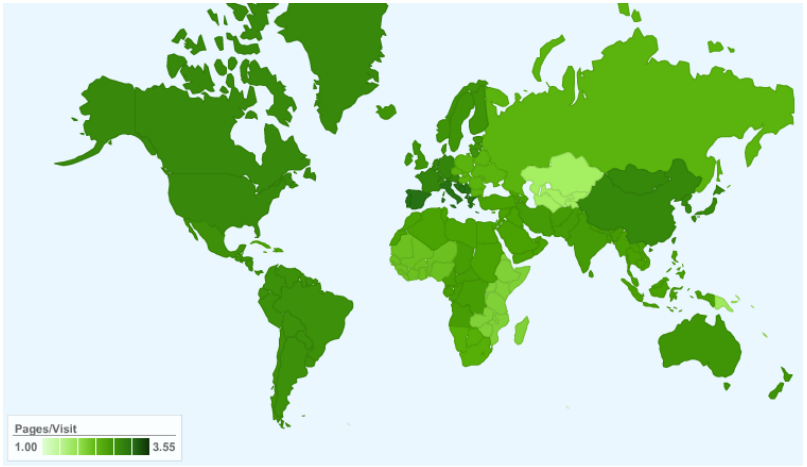


Participants

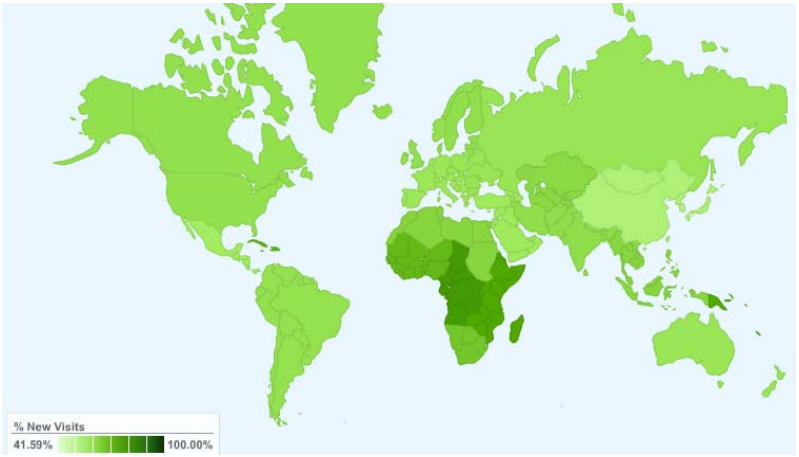
Chapters

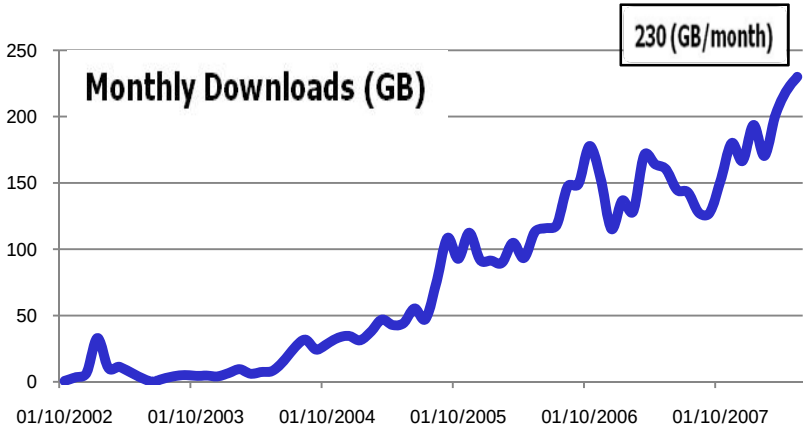
OWASP Dashboard

Worldwide Users

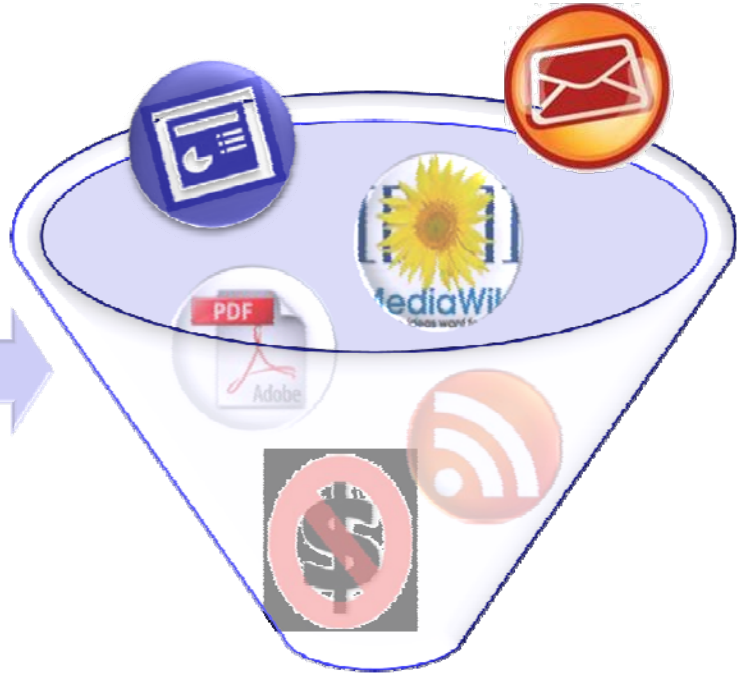


Most New Visitors





La base di conoscenza di OWASP



- 6,381 Articoli
- 427 presentazioni
- 200 aggiornamenti/giorno
- 271 mailing lists
- 180 blog monitorati

OWASP Top Ten

www.owasp.org/index.php?title=Top_10_2007

- A1: Cross Site Scripting (XSS)
- A2: Injection Flaws
- A3: Malicious File Execution
- A4: Insecure Direct Object Reference
- A5: Cross Site Request Forgery (CSRF)
- A6: Information Leakage and Improper Error Handling
- A7: Broken Authentication and Session Management
- A8: Insecure Cryptographic Storage
- A9: Insecure Communications
- A10: Failure to Restrict URL Access

OWASP
The Open Web Application Security Project
http://www.owasp.org

PCI Security Standards Council

Linee Guida OWASP

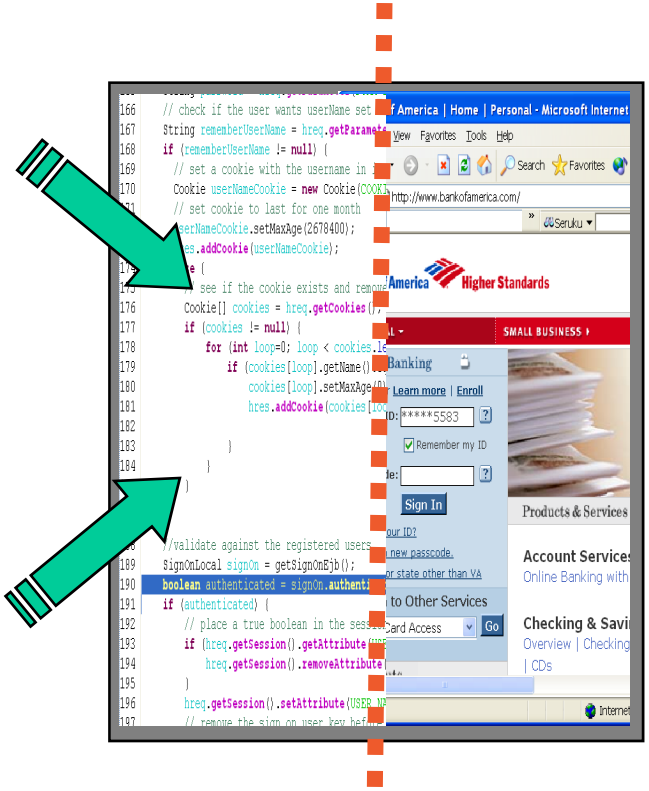
- Gratuite e open source
- Libri a basso costo
- Coprono tutti i controlli di sicurezza
- Centinaia di esperti
- Tutti gli aspetti di sicurezza applicativa

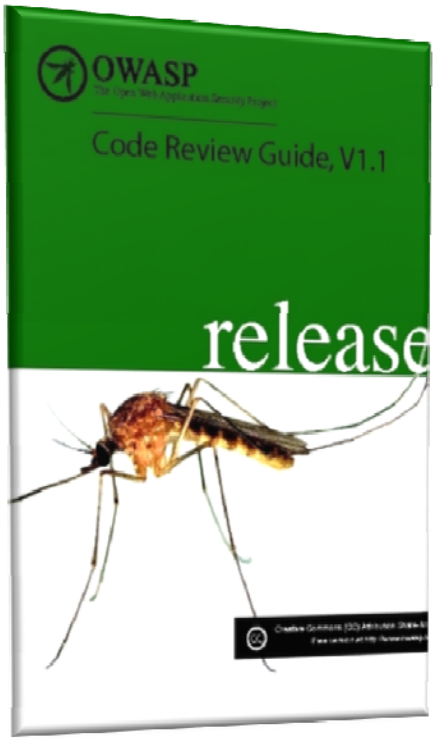
OWASP Building Guide

- Al fine di comprendere ed eliminare le cause della “insicurezza” nel software,OWASP ha sviluppato la guida per lo sviluppo delle applicazioni web sicure pensata per:
  - Sviluppatori per implementare i meccanismi di sicurezza ed evitare le vulnerabilità;
  - Project manager che la utilizzano per identificare le attività da svolgere (threat modeling, code review, development);
  - Team di sicurezza che la usano per apprendere le tematiche di application security e l’approccio per la messa in sicurezza;

OWASP Code Review Guide

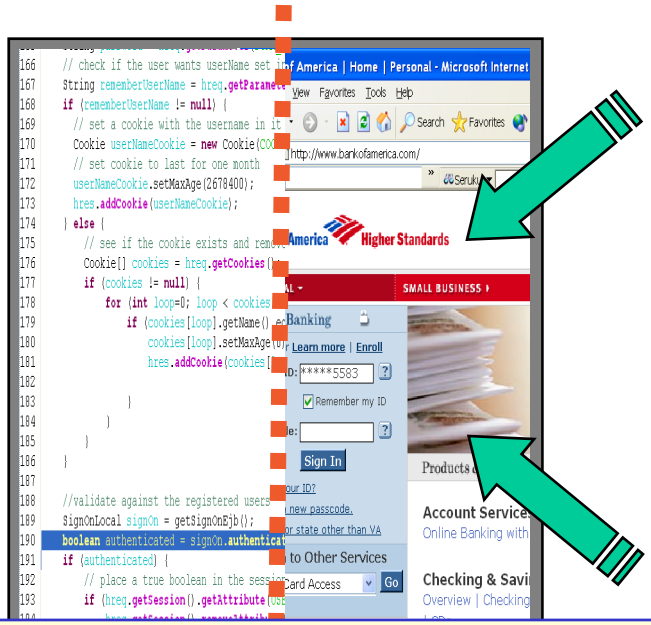
- Descrive la metodologia OWASP per testare il codice di un'applicazione (white box testing, conoscendo il codice sorgente)





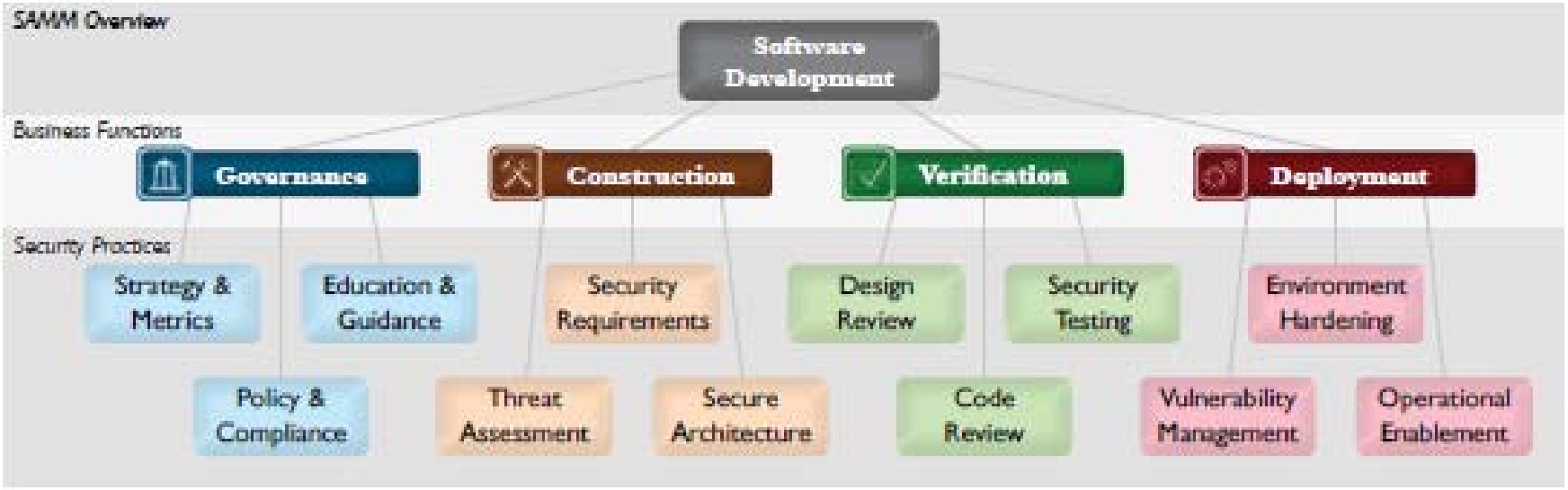
OWASP Testing Guide

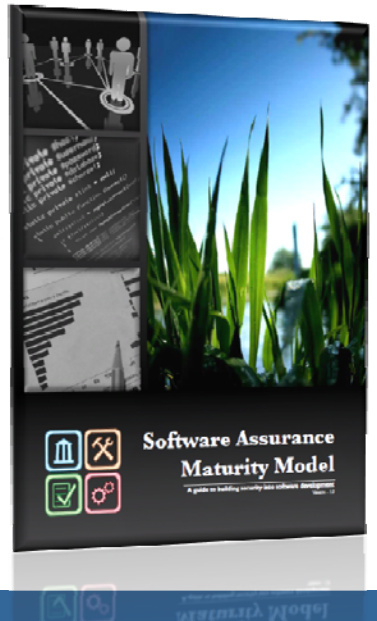
- Descrive la metodologia OWASP per testare la sicurezza di un applicativo web



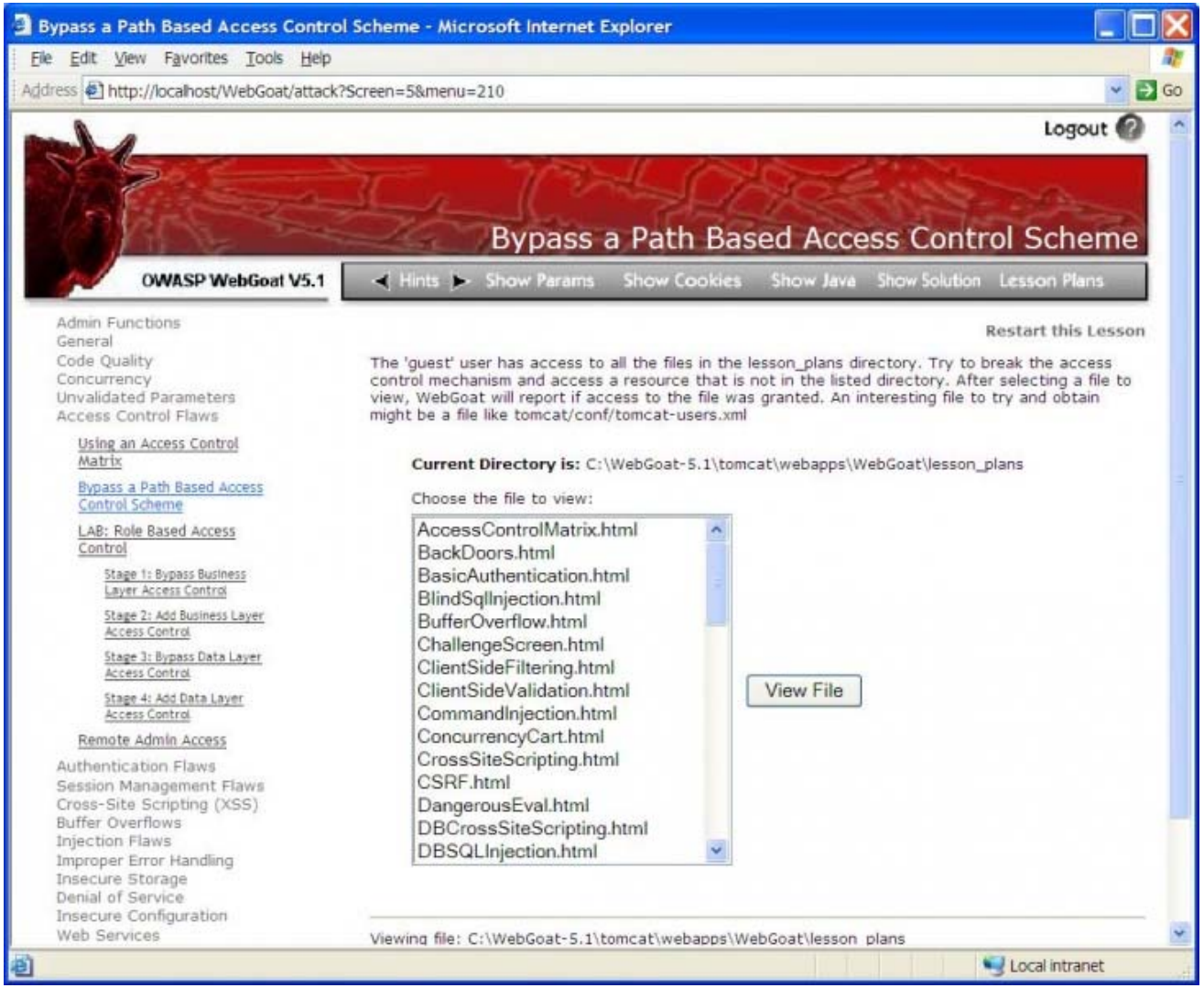
- **SANS Top 20 2007**
- **NIST "Technical Guide to Information Security Testing (Draft)"**
- **Gary McGraw (CTO Cigital) says: "In my opinion it is the strongest piece of Intellectual Property in the OWASP portfolio"**

OWASP Software Assurance Maturity Model

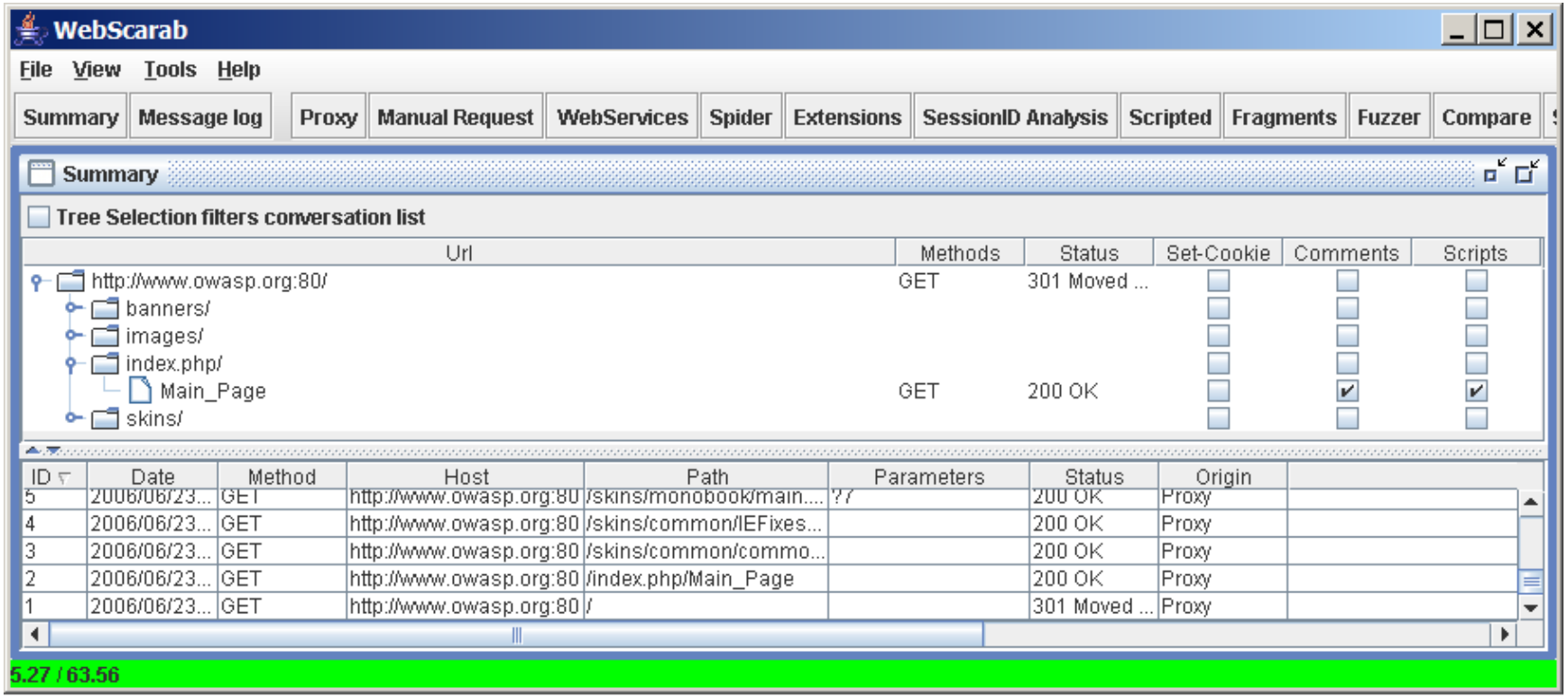




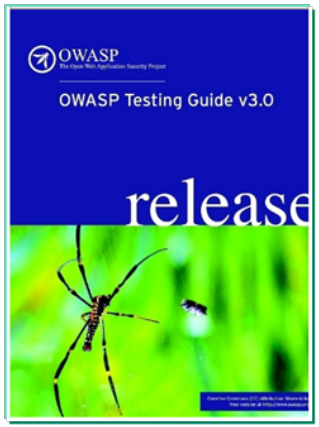
OWASP WebGoat



OWASP WebScarab

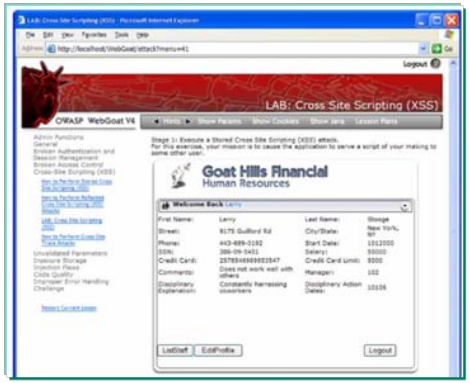


Principali progetti OWASP



BOOKS

- Owasp top10
- Building guide
- Code review guide
- Testing guide



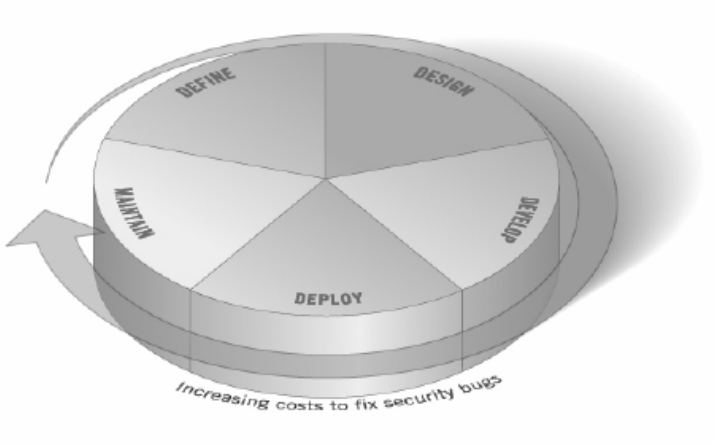
TOOLS

- WebGoat
- WebScarab
- SQLMap – SQL Ninja
- SWF Intruder
- Orizon
- Code Crawler

Il ciclo di vita del software e la sicurezza

Il ciclo di vita del software

- Il Ciclo di Vita del Software (Sofware Development Life Cycle, SDLC) comprende :
  - Define
  - Design
  - Develop
  - Deploy
  - Maintain
- Quali processi implementare?
  - Awareness
  - Secure Code Guidelines
  - Code Review
  - Application Testing



SDLC & OWASP Guidelines e tools